COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
WHITTY SOMVICHIAN (194463)
(wsomvichian@cooley.com)
KYLE C. WONG (224021)
(kwong@cooley.com)
LAUREN J. POMEROY (291604)
(lpomeroy@cooley.com)
ELLIE BARCZAK (329180)
(ebarczak@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: +1 415 693 2000
Facsimile: +1 415 693 2222

Attorneys for Defendant
Plaid Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

IN RE PLAID INC. PRIVACY LITIGATION

THIS DOCUMENT RELATES TO:

ALL ACTIONS

Case No. 4:20-cv-03056-DMR

REPLY IN SUPPORT OF PLAID INC.'S MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED AMENDED COMPLAINT

Date: TBA
Time: 1:00 p.m.
Dept: Courtroom 4 – 3rd Floor
Judge: Donna M. Ryu

Trial Date: None Set
Date Action Filed: May 4, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

I. INTRODUCTION

Plaintiffs cannot remedy the many defects of the CAC[1] set forth in Plaid's Motion to Dismiss, so their Opposition instead relies largely on mischaracterizations and hyperbole. Echoing the CAC's unfounded assertions, Plaintiffs claim, for example, that Plaid acted "surreptitious[ly]," operating "in the deep background" so that "consumers would not learn Plaid even exists." Opp. 1, 6. But these sensationalistic claims, which contradict information in the CAC and judicially-noticeable evidence, are no substitute for the well-pleaded fact allegations that Rule 8 demands. The CAC fails in its entirety for several reasons, including the following overarching defects.

First, Plaintiffs' theme of covert secrecy, which underlies all of their claims, is belied by the Plaid Link flow and Privacy Policy shown in the CAC. These materials expressly identify Plaid and explain its role in enabling consumers to link their financial accounts to their chosen apps, undermining the fundamental premise of the CAC. Plaintiffs respond by baldly misstating Plaid's disclosures and urging the Court to impose requirements the law does not mandate, but they ultimately cannot avoid the consent defense that applies to all claims.

Second, Plaintiffs fail to allege they suffered any cognizable harm for Article III purposes, let alone the specific type of economic injuries required under the CFAA, CDAFA and UCL. Plaintiffs' Opposition only underscores the hypothetical and speculative nature of their theories.

Third, Plaintiffs ask the Court to apply statutes that have nothing to do with the alleged practices at issue. For example, because the SCA applies only to unauthorized access to "facilities" that provide an "electronic communications service" ("ECS"), Plaintiffs are forced to argue their banks are ECS providers. But they are not, and the CAC alleges no facts to support such a bizarre claim. Similarly, Plaintiffs seek to impose liability under the Anti-Phishing Act ("APA"), which requires a showing that Plaintiffs were the victims of a phishing scheme that led to identity theft, caused their accounts to be hijacked, or otherwise "adversely affected" Plaintiffs in some way. The CAC alleges none of these things.

For these and other reasons, the CAC should be dismissed in its entirety, and Plaintiffs should not be given leave to amend given their many failed attempts to state a viable claim.

[1] Unless otherwise noted, defined terms have the same meaning as in the opening brief.

II. ARGUMENT

A. Plaid's Privacy Policy Bars All Claims

Plaintiffs tacitly concede that valid consent to a privacy policy precludes all claims based on practices disclosed in the policy, but try to avoid the impact of Plaid's Privacy Policy on various meritless grounds. Opp. 6. *See also* Mot. 18, 22, 27, 31, 32, 36 (discussing consent defense).

1. Consumers Were On Notice of Plaid's Privacy Policy

Plaintiffs do not contest that consumers who link their financial accounts to payment apps like Venmo[2] are presented with a screen in which they (1) must click a "Continue" button before they can link their financial accounts, (2) are advised (in text directly above the "Continue" button) that by clicking "Continue," consumers "agree to the Plaid End User Privacy Policy," and (3) can click that hyperlinked text to directly access the Privacy Policy. CAC ¶¶ 69, 71. This process constitutes consent to all practices disclosed in the Privacy Policy, which expressly addresses each of the practices alleged in the CAC.[3] Mot. 4-5. See *also In re Yahoo Mail Litig.,* 7 F. Supp. 3d 1016, 1029-30 (N.D. Cal. 2014) (finding plaintiffs consented to practices disclosed in Yahoo's privacy policy where they clicked through a sign-up screen that linked to the policy).

Plaintiffs claim the Privacy Policy is not binding because the link to it was not underlined and the font was not prominent enough. But enforceability does not turn on these details. Plaintiffs' cited cases are distinguishable because they turned on the courts' concern that cluttered consent pages confused consumers by asking them to do more than just agree to terms. In *Colgate v. JUUL Labs, Inc*., 402 F. Supp. 3d 728, 763 (N.D. Cal. 2019), the page displayed four separate text boxes for users to enter information and a "Forgot Password?" link above the link to the terms of service. The court expressed concern that users would focus on the "Forgot Password" link and

[2] Plaintiffs claim some apps differ from the Venmo process shown in the CAC, but their individual claims all involve Venmo and they cannot rely on hypothetical circumstances of consumers who used other payment apps and were not exposed to the Venmo process. *See Singh v. Google LLC*, No. 16-CV-03734-BLF, 2018 WL 984854, at *2, *5 (N.D. Cal. Feb. 20, 2018) ("the class experience cannot serve as a substitute" for allegations of plaintiffs' own experiences).

[3] The CAC alleges that Plaid sells consumers' data, which would be contrary to Plaid's Privacy Policy, but these conclusory assertions lack any factual support—because they are untrue. Indeed, Plaintiffs' Opposition backs away from these false allegations, asserting that the alleged "sale" is of "products that make Plaintiffs' data available to others," which is simply an oblique reference to Plaid's role in enabling consumers to link their financial accounts to their apps. Opp. 4-5.

not the smaller link to the terms below. *Id*. In *Applebaum v. Lyft, Inc*., 263 F. Supp. 3d 454, 467 (S.D.N.Y. 2017), the screen linking to the terms of service was titled "Add Phone Number," asked users to enter their number, and stated: "We'll send you a [text] message to verify your phone." The court found this did not give sufficient notice of defendant's terms because the "entire screen was structured as a part of a process to verify a phone number." *Id*.

Plaid's consent screen contains no such distractions. There are no fields prompting the user to enter information that might cause confusion, no other links drawing attention away from the linked Privacy Policy, and no purpose other than to obtain users' consent via the "Continue" button. In *Meyer v. Uber Technologies*, 868 F.3d 66, 78 (2d Cir. 2017), the court validated a similar flow because a nearly identically worded link to Uber's privacy policy was positioned on an "uncluttered" payment screen "directly below the buttons for registration." Here, Plaid's disclosure of its Privacy Policy is the only text in nearly half the screen and—even more prominent than in *Meyer*—is positioned directly *above* the "Continue" button. In *Peter v. DoorDash*, 445 F. Supp. 3d 580, 586 (N.D. Cal. 2020), the court similarly found that text referring to DoorDash's terms of service—which was nearly identical to Plaid's text and also placed next to the "sign up" button—"was reasonably communicated to the user," despite plaintiffs' complaint that the text was "unreasonably small" and "displayed as grey font on a lighter-shade of grey background."

Similarly here, Plaintiffs' focus on underlining and other details does not change the fact that consumers viewing Plaid's consent screen "would have known about the terms and the conduct that would be required to assent to them." *Meyer*, 868 F.3d at 77. Plaintiffs' insistence on these elements as necessary requirements for enforceability runs counter to the common understanding of privacy policies. As courts have recognized, "[t]he act of contracting for consumer services online is now commonplace in the American economy" such that "[a]ny reasonably-active adult consumer will almost certainly appreciate that by signing up for a particular service, he or she is accepting the terms and conditions of the provider." *Selden v. Airbnb, Inc*., No. 16-CV-00933 (CRC), 2016 WL 6476934, at *5 (D.D.C. Nov. 1, 2016). Against this backdrop, the alleged lack of underlined or colored text in the Plaid Link flow does not detract from the express disclosure and link that give reasonable notice to consumers that they are agreeing to Plaid's Privacy Policy.

2. Plaid's Privacy Policy Expressly Discloses How It Collects and Uses Data

In an effort to avoid the consent defense, Plaintiffs repeatedly mischaracterize the Plaid Link screens and Privacy Policy to obscure their clear disclosures. First, Plaintiffs suggest Plaid's role in linking payments apps to financial accounts is either entirely undisclosed ("it was never apparent that [Plaid] was even present," Opp. 6), or (in seeming contradiction) that Plaid's involvement *was* disclosed but the Privacy Policy does not adequately "explain what Plaid actually is" (Opp. 8). Both arguments are false, as demonstrated by Plaintiffs' own allegations and the judicially-noticeable evidence. As the CAC shows, Plaid's involvement is expressly disclosed in the Venmo flow that Plaintiffs use to illustrate their claims. CAC ¶¶ 67-71 (depicting screens that state "Venmo uses Plaid to link your bank."). Moreover, Plaid does not suggest that it is an affiliated "service of Venmo or the banks," or otherwise hide what it "actually is," as Plaintiffs claim. Opp. 6 n. 4, 8). To the contrary, the Privacy Policy makes clear Plaid's role as an independent entity, explaining that Plaid enables consumers to "connect [their] bank account and other financial accounts to software applications" and that these "software applications are built and powered by our [Plaid's] business customers …." Dettmer Decl. Ex. A at 2.

Plaintiffs also argue consumers would "expect that any 'Plaid services' used by the Apps would not collect any data beyond that needed to verify the account," emphasizing the following text from the Privacy Policy (Opp. 9): "The information we receive from the financial product and service providers that maintain your financial accounts *varies depending on the specific Plaid services developers use to power their applications,* as well as the information made available by those providers." Dettmer Decl. Ex. A at 2-3 (emphasis added). But this argument assumes payment apps only need to "verify the account" and never need additional data to enable an app's features. Plaintiffs have no basis for that assumption and allege none in the CAC. Indeed, the language Plaintiffs rely on clarifies that Plaid receives data, not just to verify accounts, but to "power [developers'] applications" more broadly. Moreover, Plaintiffs ignore the sentence immediately following their emphasized text, which further clarifies that the data Plaid receives also depends on the "information made available by providers," which can differ for different providers.

The paragraph then states: "in general, we collect the following types of identifiers, commercial information, and other personal information from your financial product and service providers," and lists eight data categories, including "Account information," "transaction history" of "credit accounts," and "Information about account transactions." *Id.* at 3. Plaintiffs make no effort to address these disclosures, which preclude their effort to misconstrue the Privacy Policy as promising that transactions data will never be collected when consumers link a payment app.

Plaintiffs' other Privacy Policy arguments are similarly unavailing, as summarized below:

Plaintiffs' Mischaracterizations	**The Privacy Policy's Actual Disclosures**
Plaintiffs claim consumers "would not understand that *their* private banking credentials and financial data were even at issue." (Opp. 8)(emphasis in text).	But the Privacy Policy states: "we collect identifiers and login information required by the provider of your account, such as *your username and password*, or a security token." Dettmer Decl. Ex. A at 2 (emphasis added).
Plaintiffs make a convoluted argument that the Privacy Policy obscures Plaid's involvement because of a provision stating Plaid obtains information on "which features within our service you access." (Opp. 8 n. 6)	But the quoted text is from the section "Information we receive *from your devices*" and has nothing to do with data that Plaid receives from *financial institutions*. Dettmer Decl. Ex A at 3 (emphasis added.)
Plaintiffs argue the words "where applicable" below mislead consumers to think Plaid does not always collect login information when it links an account. (Opp. 8-9) "When you connect your financial accounts with a developer application or otherwise connect your financial accounts through Plaid, *where applicable*, we collect identifiers and login information required by the provider of your account, such as your username and password, or a security token." Dettmer Ex. A at 2 (emphasis added).	But "where applicable" refers to the fact that some providers may not require both "identifiers and login information," and the specific information collected depends on the provider. The phrase does not undermine the clear disclosure that Plaid will collect ("we collect") whatever "identifiers and login information" are needed to link an account.

3. Plaintiffs Cannot Disclaim the Current Privacy Policy as Irrelevant

After claiming the Privacy Policy is "misleading and deceptive," Plaintiffs ask the Court to ignore it because they may have agreed to versions with different language. Opp. 6 n. 3, 8. This argument is disingenuous. Plaintiffs rely on the current Plaid Link screens and current Privacy Policy as the premise for their claims, including directly quoting the Privacy Policy at length. *See e.g.* CAC ¶¶ 67-71, 74, 95, 101. Moreover, all Plaintiffs allege that "to the extent [they] recall specific details" of the account linking process, "those details are consistent with the discussion of Plaid's interface herein," referring to depictions of the Venmo flow. *See, e.g.*, CAC ¶ 101.

Plaintiffs cannot have it both ways—they cannot rely on current materials to support their claims, yet at the same time disclaim their relevance in opposing Plaid's motion. Regardless, the prior Privacy Policy versions in place when Plaintiffs allege they linked their accounts contain the same material terms, as discussed in Plaid's Supplemental Request for Judicial Notice filed herewith.

B. Plaintiffs Lack Article III Standing As to All Claims

1. Plaintiffs' Allegations That They Linked Their Accounts Through Plaid Are Conclusory, Ambiguous, and Legally Inadequate

In addition to the dispositive consent defense, Plaintiffs' claims fail for another overarching reason: the CAC fails to establish that Plaintiffs actually linked their accounts *through Plaid* and Plaintiffs thus cannot show any of the alleged practices actually harmed them. Mot. 4. The Opposition points to several conclusory paragraphs that refer generically to Plaintiffs as "App users who linked their financial accounts using Plaid's software," (CAC ¶ 99) or claim that Plaintiffs "suffered economic damages when Plaid deceptively acquired their bank login credentials" (CAC ¶ 215). But these sorts of conclusory allegations, lacking any factual or particularized support, are insufficient to show that any individual plaintiff in fact used Plaid. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (A "particularized" injury "must affect the plaintiff in a personal and individual way."); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007) (conclusory allegations lacking "factual enhancement" are insufficient to state a plausible claim).

The allegations that Plaintiffs claim show they linked their accounts through Plaid are not only conclusory but contradicted by other allegations. Each Plaintiff alleges that "to the extent [Plaintiff] recalls specific details" on how they linked their apps, "those details are consistent with the discussion of Plaid's interface herein," *e.g.*, CAC ¶ 101, which, as the CAC describes, includes a screen expressly disclosing that "Venmo uses Plaid to link your bank," CAC ¶ 67. But in the next paragraph, each Plaintiff disavows ever seeing this screen or anything referring to Plaid. (*e.g.*, CAC ¶¶ 102). This contradiction calls into question whether Plaintiffs actually linked their Venmo accounts using the flow described in the CAC. *Johnson v. Sunrise Senior Living Mgmt., Inc.*, No. CV1600443, 2016 WL 917888, at *10 (C.D. Cal. Mar. 8, 2016) (courts "need not accept as true allegations that are contradicted … by other allegations"). Plaintiffs' alleged unawareness of Plaid

"could just as well" indicate that they linked their mobile apps through *other* methods. *Twombly*, 550 U.S. at 557 (allegations that are consistent with a plaintiff's claim but that "could just as well" support the defendant's position are insufficient to satisfy Rule 8).

Finally, the Opposition contends that micro-deposits are the "sole alternative to link a bank account" and since Plaintiffs do not allege they used micro-deposits, they must have used Plaid. Opp. 4. But the CAC neither states nor implies that micro-deposits are the only alternative to Plaid for linking accounts—nor could it, because that is simply not true—and the single paragraph Plaintiffs cite merely states that micro-deposits or direct bank log-in are "typical" methods. CAC ¶ 32. That allegation does not come close to establishing that Plaintiffs must have used Plaid to link their accounts. Moreover, Plaintiffs do not affirmatively allege they did *not* use micro-deposits. Plaintiffs ask the Court to assume this based on its absence from the CAC, but Plaintiffs cannot meet their burden under Article III through silence. Plaintiffs' failure to plead facts plausibly showing they used Plaid to link their accounts precludes Article III standing under any theory and mandates dismissal of all claims.

2. Plaintiffs' Cited Cases Do Not Support Their Claim of Economic Injury

Even setting aside the dispositive issue above, Plaintiffs' standing arguments based on supposed economic injuries fail for additional reasons. First, the Opposition claims the Ninth Circuit recognizes standing premised on "a risk of future identity theft." Opp. 14. But Plaintiffs' cited cases all involve circumstances where the data at issue *had already been compromised*. *See In re Zappos.com, Inc*., 888 F.3d 1020 (9th Cir. 2018) (finding standing where data breach victims alleged that hackers had commandeered their accounts and identities); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (finding standing where plaintiffs' social security numbers were obtained by an unknown third-party through theft of a laptop).[4] The *Zappos* Court noted the hacker had "all the information he needed to spend money in the plaintiffs' names" and specifically

[4]Plaintiffs falsely contend that *Katz v. Pershing LLC,* 672 F.3d 64 (1st Cir. 2012), cited in Plaid's brief, was contrasted with Ninth Circuit law. While the court in *Wilding v. DNC Servs.,* No. 16-61511-CIV, 2017 WL 6345492, at *1 (S.D. Fla. Aug. 25, 2017) compared *Katz* with certain Ninth Circuit cases, the court did not conclude that the two circuits' approaches were at odds, only that the facts of each case represented different ends of the spectrum from most to least speculative harm.

distinguished the allegations from the "hypothetical and conjectural [harm] . . . if no laptop had been stolen." *Id.* at 1143. Here, Plaintiffs' theory of harm, premised on a potential data breach that has not occurred and may never occur, poses precisely the speculative scenario the Ninth Circuit explained would be "hypothetical and conjectural" and cannot support Article III standing. *Id*.

Second, Plaintiffs claim they have experienced economic harm because they have already lost indemnification rights. Opp. 14. But again, as outlined in Plaid's Motion (Mot. 9), Plaintiffs' allegations are premised on a hypothetical chain of at least six events, each of which is speculative. Plaintiffs do not confront the speculative nature of each step in this chain, except the last—that banks may at some point in the future refuse to indemnify Plaintiffs for hypothetical losses because Plaid obtained their credentials. Plaintiffs claim this latter point is not hypothetical, but point only to a letter from the American Bankers Association taking the position that banks would not willingly provide the required protections of 12 C.F.R. § 1005 if login credentials were obtained by an aggregator. This issue has not been decided by any court or legislative branch (or any of Plaintiffs' financial institutions with respect to any loss by Plaintiffs, for that matter, since Plaintiffs do not allege they experienced any such loss). This scenario is a far cry from Plaintiffs' cited cases where the loss of the compensation at issue was either already established, *see Beltran v. United States*, 441 F.2d 954, 960-61 (7th Cir. 1971), or was a legal certainty, *see Singer Co. v. Super. Ct.*, 179 Cal. App. 3d 875, 890 (1986).

Third, the Opposition claims that "loss of control over one's personally identifying information constitutes a cognizable harm sufficient to confer standing." Opp. 15. But Plaintiffs' citations—to dicta in cases involving data breaches, *see In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020), the interpretation of a Georgia criminal statute, *State v. Mayze*, 622 S.E.2d 836, 841 (Ga. 2005), or allegations of diminished value of personal information, *see In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) and *Svenson v. Google Inc.*, No. 13-04080, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016)—do not support their position. Plaintiffs do not allege any data breach or diminution in the value of their information. Instead, as Plaid's cited cases show, even if Plaintiffs had alleged Plaid obtained their personal information, that alone is insufficient to show economic injury. Opp. 10-12.

3. Plaintiffs Do Not Establish Dignitary/Privacy Harms

Plaintiffs' Opposition does not even try to defend their claim of "dignitary harm." And as to privacy injuries, Plaid does not argue that privacy injuries are categorically insufficient for standing, only that the allegations pled here did not establish that Plaintiffs suffered injuries sufficient for standing. For the reasons stated in Section B.1 and in Plaid's Motion, Plaintiffs have not established a "concrete and particularized" invasion of privacy.

C. Plaintiffs' Invoked Exceptions to the Statutes of Limitations Do Not Save Their Untimely Claims

Plaintiffs do not dispute that it has been more than two to four years since most Plaintiffs signed up to use the apps described in the CAC, a period which exceeds the statutes of limitation for some or all of those Plaintiffs' claims. Opp. 16-17. Instead, Plaintiffs argue the continuous accrual doctrine, discovery rule, and fraudulent concealment theory make their claims timely. Plaintiffs, however, cannot meet their burden to establish, nor have they adequately pled, any of these exceptions.

As Plaintiffs' own authority shows, the continuous accrual doctrine only applies "[w]hen an obligation or liability arises on a recurring basis." *Aryeh v. Canon Bus. Sols., Inc.,* 55 Cal. 4th 1185, 1199 (2013). California courts generally limit the doctrine to claims involving periodic payments or installment contracts. *See, e.g., State ex rel. Metz v. CCC Info. Servs., Inc*., 149 Cal. App. 4th 402, 418 (2007) (holding that the continuous accrual doctrine does not apply where "[the plaintiff's] action does not involve a recurring obligation or any such period payment obligations"); *Brodsky v. Apple Inc*., 445 F. Supp. 3d 110, 136–37 (N.D. Cal. 2020) ("[W]hen an alleged duty 'bears little relation to the monthly payments or monthly bills that California courts have found to be periodic, recurring obligations,' applying the continuous accrual doctrine is unwarranted.").

Plaintiffs do not allege any monthly payment or other recurrent obligation. Instead, they argue the harm is ongoing because Plaid allegedly updates its cache of data on a regular basis.[5] Opp. 16. The continuous accrual doctrine, however, does not apply so broadly. *See Brodsky*, 445

[5]Plaintiffs' Opposition also claims that the CAC alleges Plaid's monetization of the data on some regular interval. But in fact, the CAC only generally alleges monetization of the data and does not specify that this is done at any particular interval. *See* Opp. 16 (*citing* CAC ¶¶ 59-65).

F. Supp. 3d at 137 (plaintiffs' allegation that defendant continued to violate the CFAA based on software that slowed down the log-in process was not a recurring obligation and continuous accrual doctrine did not apply). The gravamen of Plaintiffs' claims (had they adequately pled them) is that Plaid obtains bank log-in information without adequate disclosures. This alleged wrong is complete at a discrete point in time—when a user provided their credentials—and is not the type of recurring obligation needed to invoke the continuous accrual doctrine. *See, e.g.*, *IV Sols., Inc. v. Connecticut Gen. Life Ins. Co*., No. CV 13-9026-GW(AJWX), 2015 WL 12516742, at *5 (C.D. Cal. Apr. 9, 2015) (continuous accrual doctrine did not apply to claims which sounded in fraud because any fraud claim would have been complete at a discrete point in time before the limitations period); *cf. Factory Direct Wholesale, LLC v. iTouchless Housewares & Prod., Inc*., 411 F. Supp. 3d 905, 918 (N.D. Cal. 2019) ("Defendant's continuing obligation to avoid illegal behavior that violates the UCL is also not a periodic, recurring obligation.").

Plaintiffs also attempt to invoke the discovery rule and the fraudulent concealment doctrine but the CAC does not support those theories. A plaintiff seeking to invoke the discovery rule must "specifically plead" the "time and manner of discovery." *Grisham v. Philip Morris U.S.A., Inc*., 40 Cal. 4th 623, 638 (2007). Similarly, the fraudulent concealment doctrine requires allegations of: "(1) when the fraud was discovered; (2) the circumstances under which it was discovered; and (3) that the plaintiff was not at fault for failing to discover it or had no actual or presumptive knowledge of facts sufficient to put him on inquiry." *Keilholtz v. Lennox Hearth Prod. Inc.*, No. C 08-00836 CW, 2009 WL 2905960, at *5 (N.D. Cal. Sept. 8, 2009) (quotation omitted). Because the CAC does not allege when or how Plaintiffs discovered the alleged wrongs,[6] Plaintiffs cannot rely on either the discovery rule or the fraudulent concealment doctrine. *See Hellgren v. Providential Home Income Plan Inc.*, No. C 06-04728 MHP, 2006 WL 8447964, at *4 (N.D. Cal. Oct. 26, 2006) (rejecting the discovery rule where plaintiffs failed to plead how and when they discovered the violation) *aff'd*, 291 F. App'x 70 (9th Cir. 2008); *Keilholtz*, 2009 WL 2905960, at

[6]The Opposition claims that Plaid's "allegations make clear that they did not uncover Plaid's misconduct until recently." Opp. 17 (citing CAC ¶ 241). But in fact the cited paragraph only claims that Plaintiffs "were ignorant of the information essential to pursue their claims" and does not "specifically plead" the "time and manner of discovery" as required.

*5 (rejecting discovery rule and fraudulent concealment doctrine where Plaintiffs failed to plead the time and manner of discovery). Moreover, any claim of delayed discovery is implausible here, given Plaid's public disclosures in its Privacy Policy. *See Iorio v. Allianz Life Ins. Co. of N. Am.*, No. 05CV633 JLS CAB, 2008 WL 8929013, at *7 (S.D. Cal. July 8, 2008) (rejecting application of the discovery rule because the contract should have put plaintiff on notice of his claims).

D. Plaintiffs Do Not Show That Their Equitable Claims Are Non-Duplicative of Their Available Legal Remedies

Plaintiffs' Opposition does not show why the numerous actions at law they have pled—invasion of privacy, Cal. Constitution Art. I, CFAA, CDAFA, SCA, Anti-Phishing Act, Cal. Civ. Code 1709, 1710—are insufficient to provide the relief they seek.[7] Via those legal claims, Plaintiffs may pursue an injunction, actual damages, treble damages, and hefty statutory penalties (although Plaid denies that Plaintiffs are entitled to any relief for all the reasons identified herein). Plaintiffs provide no reason why additional restitution and disgorgement remedies under the UCL and unjust enrichment[8] claims are necessary to make them whole. *See Franklin v. Gwinnett Cty. Pub. Sch.*, 503 U.S. 60, 75-76 (1992) ("a court should determine the adequacy of a remedy in law before resorting to equitable relief"). Instead, Plaintiffs argue the adequacy of their legal remedies will depend on "the resolution of questions regarding Plaid's profits, revenues, competitive advantage, and other valuable benefits derived from Plaintiffs' and Class members' data, and concerning the extent and manifestations of the harm Plaid has caused." Opp. 18. But Plaintiffs do not explain how any of these factors would determine the adequacy of their legal remedies. Plaintiffs claim that Plaid's authority is "distinguishable," and "against the weight of authority," but cite mostly out-of-district cases in support of that argument and fail to address the vast majority of cases cited in Plaid's Motion. Mot. 16-17. In fact, just this month another Northern District judge dismissed equitable claims because the plaintiffs had an adequate remedy of law. *Williams v. Apple, Inc.*, No. 19-CV-04700-LHK, 2020 WL 6743911, at *9 (N.D. Cal. Nov. 17, 2020). In doing so, the *Williams*

[7]With this argument, Plaid only seeks the dismissal of Plaintiffs' equitable claims, not all equitable remedies Plaintiffs may pursue through their legal claims. To the extent the Motion requested dismissal of all equitable remedies, Plaid withdraws the request.

[8]Plaintiffs concede that their declaratory relief claim (Count 4) should be dismissed as a standalone cause of action. Opp. 19, n.19.

court found that this approach was supported by Ninth Circuit law and rejected the same argument Plaintiffs advance here—that *Astiana v. Hain Celestial Grp., Inc*., 783 F.3d 753 762-63 (9th Cir. 2015) rejected the early dismissal of duplicative equitable claims.

E. Plaintiffs Fail to Address The Defects in Their SCA Claim

With respect to the statutory claims in the CAC, Plaintiffs' Opposition repeatedly attempts to contort the referenced statutes to fit circumstances they were never intended to address. First, the SCA addresses only unauthorized access to a "facility through which an electronic communications service is provided" 18 U.S.C. § 2701(a), and does not cover alleged access to account information stored at financial institutions. In an effort to shoehorn this case into the SCA, Plaintiffs insist that their banks provide an ECS because they send statements and other communications to account holders and account holders can access banking information online. Opp. 36. But the mere fact that an entity communicates electronically with its own customers does not somehow make it a provider of "an electronic communications service." *See Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001) (holding that Amazon is "not an electronic communications service provider" and rejecting plaintiff's argument that "because [Amazon] receives electronic communications from its customers," the SCA applies); *Cent. Bank & Trust v. Smith*, 215 F. Supp. 3d 1226, 1228-9, 1234 (D. Wyo. 2016) (holding that unauthorized access to "customer details" stored on a bank's "secured computer network[]" was not actionable under the SCA because the bank was not "an electronic communications service provider"); *U.S. v Standefer*, No. 06-CR-2674-H, 2007 WL 2301760, at *4 (N.D. Cal. Aug. 8, 2007) (an online payments company that "utilizes the ability to send or receive communications" is "not a service which provides users the ability to send or receive electronic communications").

Plaintiffs' own cases confirm that an ECS must involve something more than an entity simply communicating with its own customers or users. The two cases Plaintiffs cite for the proposition that their banks provide electronic communications services (Opp. 36) both involved communications that Facebook users sent to each other using Facebook's communications tools, not communications from Facebook to its users. *See Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 665 (D.N.J. 2013) (finding that Facebook is an electronic

communications provider because "Facebook provides its users with the ability to send and receive electronic communications" among each other); *Decoursey v. Sherwin-Williams Co.*, 2020 WL 1812266, at *7 (D. Kan. Apr. 9, 2020) (involving "private Facebook communications" among users). The communications Plaintiffs rely on here are not remotely similar because they consist solely of communications between banks and their customers. If that were the criteria for providing an ECS, a host of entities would be swept into the SCA's coverage that could not possibly have been intended—even federal courts would be ECS providers because they send and receive communications (pleadings) with litigants.

Second, Plaintiffs concede they must demonstrate unauthorized access to data stored "for purposes of backup protection" (18 U.S.C. § 2510(17)(B)) and argue the data at issue meets this requirement. CAC ¶ 305. But data is considered "for purposes of backup protection" only if there is some *other, primary* copy of the data, which Plaintiffs do not allege. Their cited cases confirm this rule. In *Cline v Reetz-Laiolo*, 329 F. Supp. 3d 1000 (N.D. Cal. 2018), the court held that emails stored by a provider of a web-based email service were not stored for "purposes of backup protection" because "there is no other version of the email that is being backed up" and the plaintiffs did not allege they "used their web-based email accounts 'for purposes of backup' …." *Id*. at 1046. In *U.S. v Weaver*, 636 F. Supp. 2d 769, 772 (C.D. Cal. 2009), the court examined Ninth Circuit law applying the SCA to an ISP-based email service, and explained this result "relies on the assumption that users download emails from an ISP's servers to their own computers." The ISP's copy thus is a "backup" to the primary copy that users keep on their own computers and the SCA can apply.

The account data at issue here is analogous to the web-based email at issue in *Cline* and unlike the ISP-based email in *Weaver*. Plaintiffs allege that their financial institutions "store historical communications regarding customers' past banking activities … *so that they may be accessed by consumers* …" CAC ¶ 305 (emphasis added). Critically, Plaintiffs do not allege they ever downloaded this data to store it on their own computers, or otherwise state any facts plausibly demonstrating that the data is stored anywhere other than at their banks. Given that omission, the data maintained by Plaintiffs' banks cannot be deemed a "back up" to some other, primary data storage, and their SCA claim necessarily fails. *See Theofel v Farey-Jones*, 359 F.3d 1066, 1077

(9th Cir. 2004)("A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purpose.").[9]

F. The Anti-Phishing Act Does Not Apply to Plaintiffs' Claims

Plaintiffs' arguments regarding the Anti-Phishing Act are equally meritless. First, Plaintiffs do not meaningfully address the legislative purpose of statute, which is aimed at illicit conduct. Plaintiffs vacillate between urging the Court to ignore the legislative history (Opp. 40) and cherry-picking aspects of it that they say require an expansive reading of the statute (*id*. at 41). Of course, reference to the Act's legislative history *is* critical to ensure the statute is applied consistently with its purpose. *See Kearney v Salomon Smith Barney, Inc*., 39 Cal. 4th 5, 119 (2006) (looking to the "legislatively prescribed purpose" of the California Invasion of Privacy Act to determine its scope). Plaintiffs' own cited authority recognizes as much. Opp. 41 (citing *Pineda v. Williams-Sonoma Stores, Inc*., 51 Cal. 4th 524, 532 (2011) and quoting its statement that statutes should be construed "in favor of their protective purpose.").

Here, the most relevant aspect of the legislative history is the definition of what constitutes "phishing," which frames the entire purpose of the Act. As explained throughout the legislative history that Plaintiffs attach, "phishing" involves "a widespread technique for obtaining personal information" that "is used to facilitate identity theft and other crimes" and involves "fraudulent emails or Web sites …." (Geman Decl., Exs. 2, 3, 4, 6, 7.) Here, Plaintiffs do not claim, even in their most sensationalistic allegations, that Plaid's practices are "used to facilitate identity theft and other crimes" or involve "fraudulent emails or websites." Indeed, Plaintiffs concede Plaid's "primary service" is "bank 'linking' and verification," and this service "is important for the safety and security of payment transfers using mobile apps." CAC ¶ 32. While Plaintiffs complain about how Plaid implements its services, these allegations do not amount to "phishing" by any stretch.

Plaintiffs do not directly contest the definition of what constitutes "phishing" and argue instead that the statute can be applied to "legitimate businesses." Opp. 40. But Plaid does not contend that businesses with some legitimate aspect can never violate the statute. Rather, Plaintiffs'

[9] Plaintiffs' consent, as discussed in Section II.A, also provides a complete defense under the SCA. Plaintiffs do not contest that consent to an alleged access precludes SCA liability.

claim fails because it targets only legitimate business *activity* that has nothing to do with the sort of illicit activity that is the focus of the statute. Plaintiffs' own cited authorities prove the point, by contrast. *See* Opp. 40. In *Facebook v Fisher*, defendants sent "7.2 million spam messages to Facebook users" that "trick[ed] users into divulging their Facebook login information" for the purpose of "send[ing] spam messages to the users' friends, repeating the cycle." No. C 09-05842, 2011 WL 250395, at *1 (N.D. Cal. Jan. 26, 2011). *See also Greenwich Ins. Co. v Media Breakaway LLC*, 2009 WL 6521581, at *2 (June 11, 2009 C.D. Cal.) (involving a similar scheme and defining "phishing" as "a more insidious form of solicitation [as compared to spam] whereby a person usually is lured by deceit into giving up personal information and passwords that permit the recipients to 'hijack'the account"). Plaintiffs claim the defendants in these cases were "otherwise legitimate marketing companies" (Opp. 40), but the conduct at issue was certainly not "legitimate" and Plaintiffs do not argue (nor could they) that the circumstances here are remotely similar.

Second, and relatedly, Plaintiffs do not meaningfully address the Act's "adversely affected" requirement. Plaintiffs say they meet this requirement by alleging "Plaid acquired their private information under false pretenses," (Opp. 40), but that merely restates the liability requirements of Section 22948.2. Section 22948.3 imposes an additional requirement that civil claimants must be "adversely affected," and this independent provision must be given effect. *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (the canon against surplusage counsels that courts should give effect to each word or provision in a statute). To Plaid's knowledge, every published decision finding Anti-Phishing Act liability (including Plaintiffs' cited cases above) has involved a plaintiff who was "adversely affected" in the ways the statute was meant to prevent, generally involving identity theft, hijacking of accounts, or similar harms. *See, e.g.*, *Facebook v. Wallace,* No. C 09-798 JF (RS), 2009 WL 3617789, at *2 (N.D. Cal. Oct. 29, 2009) (defendants obtained Facebook log-in credentials and hijacked accounts to send automated messages that appeared to originate from the user); *MySpace, Inc. v. Wallace*, 498 F. Supp. 2d 1293, 1298 (C.D. Cal. 2007) (same). No published decision to Plaid's knowledge has found that a plaintiff was "adversely affected" based on the types of abstract and speculative "harms" on which the CAC is based.

Third, Plaintiffs do not meaningfully address their failure to allege Plaid acted "without …

authority" from financial institutions. Mot. 34. Plaintiffs point to articles about industry-wide issues and unrelated litigation. Opp. 39. But Plaintiffs cannot rely on generalized allegations that, by their own characterization, relate only to "[s]ome banks" (CAC ¶ 80), without alleging facts about their *own* circumstances. *See Singh*, 2018 WL 984854, at *5 (a complaint must be based on the plaintiff's "personal experience" and "the class experience cannot serve as a substitute").

G. Plaintiffs' CFAA And CDAFA Claims Fail For Multiple Reasons

1. Damages Cannot Be Aggregated To Meet CFAA's $5,000 Threshold

Plaintiffs' CFAA claims fare no better than their other statutory claims. First, Plaintiffs contend they meet the "economic damages" threshold because damages can be aggregated for all putative class members, and the lost value of indemnification rights exceeds $5,000. Opp. 27-28. Neither are true. Courts have made clear that plaintiffs can aggregate classwide damages under the CFAA only where a single unified act was applied to all putative class members. *Compare In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *11 (N.D. Cal. Sept. 20, 2011) (no aggregation permitted where consumers alleged they voluntarily installed an unspecified number of third party apps which allegedly used their personal information without consent), *with In re Apple & AT&TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008) (defendant propagated a single software update to all users); *Creative Computing v. Getloaded.com LLC,* 386 F.3d 930, 934-36 (9th Cir. 2004) (defendant accessed identical information in the same manner multiple times). Plaintiffs' allegations here do not come close to meeting this requirement. Unlike Plaintiffs' cited cases, the CAC involves multiple, discrete events implicating "a vast array of popular consumer-facing mobile and web-based fintech apps" by consumers over a seven year period. CAC ¶ 31. Further, Plaintiffs allege that each putative class member's financial information was obtained by Plaid on an individual basis, from "over 11,000" individual financial institutions. CAC ¶¶ 58, 103, 113, 124, 133, 143, 153,162,171, 181, 192, 202. This is simply not "the same act" by the defendant contemplated by the CFAA.

Second, the alleged loss of indemnification rights is entirely speculative, as explained in Section B.2, and thus cannot support the CFAA's damages threshold. *Vecchio v. Amazon.com Inc.*, No. C11-366-RSL, 2011WL 6325910, at *3 (W.D. Wash. Dec 1, 2011) ($5,000 CFAA threshold

not met where plaintiffs' allegation of loss was "entirely speculative").

2. Plaintiffs Allege No "Damage" Or "Loss"

Plaintiffs argue that they have pled "damage" (CFAA (a)(5)(A)-(C)) and "damage or loss" (CDAFA),[10] required under each statute because they have pled "impairment to the integrity of their data" or to the "integrity of the system." But none of their authority stands for the proposition that simply copying Plaintiffs' data from one place (the banking institution) to another (Plaid's servers) impairs the integrity of either data or systems.[11] According to Plaintiffs' own cases, the "term 'integrity' in the [CFAA] to define damage requires 'some diminution in the completeness or usability of data or information on a computer system.'" *Satmodo, LLC v. Whenever Communications*, *LLC*, 2017 WL 6327132, at *4 (S.D. Cal. Dec. 8, 2017). There is no comparable allegation here that Plaintiffs' financial data has itself lost value.[12] Plaintiffs attempt to distinguish Plaid's cited cases on the basis that Plaid allegedly accessed class members' data on a regular basis, but this is a distinction without import. Unlike the authority Plaintiffs cite, Plaid's access did not impact the integrity of any banking system by "install[ing] a program on the target computer." *U.S. v. Yücel*, 97 F. Supp. 3d 413, 421 (S.D. NY 2015); *see also Microsoft Corp. v. Mutairi*, 2015 U.S. Dist. LEXIS 95541, at *3 (D. Nev. June 25, 2015) (allegation that defendant installed malware); *Microsoft Corp. v. Doe*, No. 14-00811, 2015 WL 4937441, at *9 (E.D. Va. Aug. 17, 2015) (same).[13]

---

[10] Plaid's Motion also argued that Sections 502(c)(1) and (c)(4) of the CDAFA are subject to a higher standard. Plaintiffs' only rebuttal—that the CDAFA should be interpreted consistently with the CFAA—is contradicted by the differing language of the statutes. *U.S. v. Christensen,* 828 F.3d 762 789 (9th Cir. 2015) (recognizing differences between the laws and applying each statute individually).

[11] Plaintiffs argue that Plaid's integration on the apps they voluntarily installed damaged their smartphones. Opp. 30. That proposition has been explicitly rejected as to the CDAFA. *See Flextronics Int'l, Ltd. v. Parametric Tech. Corp*., No. 5:13-CV-00034-PSG, 2014 WL 2213910, at *4 (N.D. Cal. May 28, 2014). Moreover, as to both laws, Plaintiffs failed to allege that the third-party app impaired the integrity of their smartphones or caused damage to smartphone data.

[12] Plaintiffs' contention that moving data from a banking system to Plaid's systems caused damage has been rejected. See *NetApp, Inc. v. Nimble Storage, Inc*., No. 5:13-CV-05058-LHK (HRL), 2015 WL 400251, at *14 (N.D. Cal. Jan. 29, 2015).

[13] Plaintiffs cite *Shurgard Storage Centers, Inc., v. Safeguard Self Storage, Inc*., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) for the proposition that simply copying data damages its integrity, but *Shurgard* involved a trade secret, which lost value when it was obtained and used by a competitor. Plaintiffs also cite *Therapeutic Research Faculty v. NBTY Inc*., 488 F. Supp. 2d 991 (E.D. Cal. 2007), but the conclusory reasoning in that case has been rejected by other courts in this district. *See NetApp,* 2015 WL 4000251, at *12-15 (rejecting the reasoning of both *Shurgard Storage* and *Therapeutic Research* and concluding the copying data did not constitute damage under the CFAA).

3. Plaintiffs Do Not Plead Contaminant/Transmission of a Program

Plaintiffs' Opposition does not contend that anything Plaid transmitted or placed on any banking system constitutes a "contaminant" (CDAFA § 502(c)(8)) or the "transmission of a program, information, code, or command" (CFAA § 1030(a)(5)(A)). Instead, Plaintiffs contend that Plaid's integration into the apps they voluntarily installed satisfies both statutes. Opp. 35. But Plaid's integration is not like the code that operated in the one case Plaintiffs cite, *Flextronics*, 2014 WL 2213910, at *6, in which hidden software operated to transmit information to the defendant, unbeknownst to the plaintiff. Here, as the CAC shows, the process of linking through Plaid a financial account to an app like Venmo requires consumers to knowingly enter their credentials for the express purpose of transmitting those credentials. CAC ¶ 38-39. This is insufficient under CFAA § 1030(a)(5)(A) which requires pleading "transmission of . . . code . . . [that] as a result of such conduct, intentionally causes damage without authorization," because (1) Plaintiffs authorized transmission of their credentials and (2) no damage is alleged to Plaintiffs' smartphones. Nor is it adequate under CDAFA § 502(c)(8), because Plaintiffs have not pled "that the actions of the contaminant (modify/damage/destroy/record/transmit) were undertaken by overcoming a technical barrier without the permission of the owner." *Flextronics Int'l,* 2014 WL 2213910, at *5.

4. Plaintiffs' Do Not Establish Credential Trafficking

Plaintiffs' Opposition argues that the CAC pleads credential trafficking because Plaid (1) "obtain[ed] 'access tokens or similar information from Plaintiffs' and Class members' financial institutions" or (2) "transferr[ed] to the Participating Apps access tokens or similar information from Plaintiffs' and Class members' banks." Opp. 33. But the CAC does not adequately allege either. The CAC references "access tokens," only to unjustifiably criticize Plaid because *it did not use the OAuth process wherein tokens are used*. CAC ¶ 33-35. Plaintiffs concede that the CAC alleges the Plaid Link screen for apps like Venmo includes the statement "login credentials will not be made accessible to Venmo," but claim the CAC also alleges this statement is misleading and thus is not probative of whether Plaid actually transfers credentials. Opp. 33. But the CAC only contends that Plaid's statement provided users a false sense of security, not that it was false as to Venmo's access to credentials. CAC ¶ 74(b). Given the CAC's allegations that Plaid obtains

credentials directly and no longer uses a process whereby the fintech client would also get access to the credentials (CAC ¶¶ 34, 35, 39, 45), the contradictory and conclusory sentences made solely to state the required elements of this claim should be rejected as implausible.[14]

H. The UCL Claim Fails Along With Plaintiffs' Other Claims

Plaintiffs' failure to allege economic harm, which plagues the CAC as a whole, also precludes liability under any of the UCL's prongs. Plaintiffs' theory—that their banks *might* not indemnify them for financial losses that *may* occur in the future *if* their data is compromised—is far too speculative because the UCL requires "a loss or deprivation of money or property" that is "concrete and particularized," not merely "conjectural or hypothetical." *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1048-9 (9th Cir. 2017) (quotation and citations omitted). Even where a consumer's data has *actually* been compromised, the threat of future harm is not sufficient. *See Bass v. Facebook, Inc*., 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (finding allegations of future risk in connection with data breach insufficient to establish UCL standing). Plaintiffs' theory of economic harm is even more attenuated, *see* Section A.2, and has no support in the case law. The only case Plaintiffs cite underscores Plaid's point. *See Gonzales v. Uber Techs., Inc.,* 305 F. Supp. 3d 1078, 1093 (N.D. Cal. 2018) (allowing UCL claim to proceed where plaintiff "sufficiently alleged that he lost revenue" from the alleged practices). There are no similar allegations here to show that Plaintiffs suffered any *present* economic loss.

Additionally, Plaintiffs do not allege a predicate unlawful act as needed for the UCL's unlawful prong. Plaintiffs point out that a violation of a statute with no private right of action can support an unlawful prong claim. But that rule is subject to an exception where the statute expressly vests exclusive enforcement with a governmental body, in which case "a litigant may not rely on the proscriptions of [the statute] as the basis for a UCL claim." *See Zhang v. Super. Ct.*, 57 Cal. 4th 364, 384 (2013). Plaintiffs do not contest this rule.[15] Nor do they contest that the GBLA and

[14]For the reasons explained in Section A., consumers' consent to Plaid's Privacy Policy information precludes any showing that Plaid's actions were "without permission," (CDAFA), or "without authorization, or exceed[ed] authorized access" (CFAA).

[15] In Plaintiffs' only cited case, *In re Anthem Data Breach Litig.,* the UCL unlawful prong violation was based on alleged violations of seven different statutes and the did not specifically address the GBLA. 162 F. Supp. 3d 953, 989 (N.D. Cal. 2016).

CalFIPA expressly bar private enforcement. Mot. 20. Moreover, Plaintiffs cite no authority for their theory that CalOPPA applies to all individuals hypothetically interested in "seeking" goods or services. Opp. 24. Rather, § 22577 requires that the consumer intends to pay "by purchase or by lease" for such goods or services. Plaintiffs allege no such thing. Cal. Bus. Prof. Code § 22577.[16]

Last, Plaintiffs' UCL claim fails because Plaintiffs do not allege reasonable reliance. Plaintiffs argue that it suffices for them to say they would not have linked their accounts had they known of Plaid's involvement and how it collects data. Opp. 26. But Plaintiffs' alleged ignorance of facts disclosed in the linking process and in Plaid's Privacy Policy cannot support a claim under the UCL's fraudulent or unfair prongs. *See Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1163 (9th Cir. 2012) (no reasonable reliance where plaintiff "had a reasonable opportunity to discover the true terms of the contract"); *Meyer v. Aabaco Small Bus., LLC*, No. 5:17-cv-02102-EJD, 2018 WL 306688, at *3 (N.D. Cal. Jan. 5, 2018) (dismissing UCL claim where plaintiff failed to allege reliance on an affirmative misrepresentation and defendant's terms disclosed the allegedly wrongful practice); *cf. Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1126-27 (9th Cir. 2009) (a court is not required to "separately analyz[e] [the plaintiff's] claims under the unfairness prong of the UCL" where the "unfair" claim is based on the same facts as the "fraudulent" claim).

I. Plaintiffs' Cited Cases Do Not Support Their Invasion of Privacy Claims

Plaintiffs' Opposition fails to rebut Plaid's showing that Plaintiffs do not satisfy the elements of their invasion of privacy and California Constitution Article I claims. First, Plaintiffs did not have a reasonable expectation of privacy in any financial data allegedly acquired by Plaid, not because financial data is not private, but because Plaintiffs all claim to have used Venmo, which utilizes a flow that requires agreement to Plaid's Privacy Policy as shown in the CAC. Mot. 32. Plaintiffs' Opposition fails to address the impact of these facts on a reasonable expectation of privacy, instead citing non sequitur cases for the general and basic proposition that financial data is private (which Plaid does not dispute). *See United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (addressing Fourth Amendment challenge to border search of laptop computer); *Cal.*

[16]Plaintiffs do not address Plaid's arguments that (1) CalOPPA only covers information from California customers, or (2) that Plaid's policy is compliant with the applicable standards for an online service provider under Sec. 22577(b)(5).

Bankers Ass'n v. Shultz, 416 U.S. 21, 89-90 (1974) (quoting from dissenting opinion on constitutionality of provisions of the Bank Secrecy Act); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting Fourth Amendment jurisprudence in support of Article III standing holding). None of these cases is remotely relevant to the facts here, where Plaintiffs acknowledge that Plaid's Privacy Policy discloses that Plaid collects "Information about account transactions, including amount, date, payee, type, quantity, price, location, involved securities, and a description of the transaction." CAC ¶ 71.

Similarly, Plaid's Motion argued that Plaintiffs could not show an "egregious breach of the social norms" simply by alleging that Plaid acquired data and that Plaid's privacy policy was ambiguous or insufficiently prominent. Mot. 32-33. Plaintiffs' Opposition offers no rebuttal. Instead, Plaintiffs claim without support that Plaid's conduct "violate[s] industry norms." Opp. 22. But citations to the CAC allege the opposite—that Plaid's practices are purportedly in line with those of other data aggregators. CAC ¶ 79.[17] Plaintiffs also argue that the alleged conduct is egregious because it is characterized by "deceit," but Plaintiffs' self-serving statements that Plaid "represent[ed] itself to be trusted financial institutions and hid[] its involvement as a third-party" (Opp. 22) are belied by their own allegations, as discussed above. *See* Section A. In contrast, the "deceit" described in the cases Plaintiffs cite involves alleged conduct that contradicted the defendant's applicable policy disclosures, which Plaintiffs do not allege here (nor can they). *See In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 606 (9th Cir. 2020) (alleging Facebook collected the very information that its privacy policy explicitly denied collecting); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 150-51 (3d Cir. 2015) (using covert means to set cookies on browsers with cookie-blocking features despite assuring users in its Privacy Policy that such browsers would block third-party cookies); *In re Vizio Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (collecting consumer video history despite assuring consumers they could turn such sharing "Off").

[17] Plaintiffs also contend Plaid violated industry norms, citing to various provisions of the Gramm Leach Bliley Act that are inapplicable for the reasons noted in Plaid's Motion. Mot. 20 n.1. Even if they applied, and even had Plaid failed to comply with them, this is simply Plaintiffs' original allegations of inadequate notice repackaged as an "industry norm." Plaintiffs provide no support for the allegation that allegedly inadequate notice should be equated with egregious conduct.

Plaintiffs' attempt to distinguish the cases cited by Plaid on the basis that the data obtained in those cases was not as sensitive as the data at issue here also fails. Plaintiffs' implicit argument—that the sensitivity of the data is determinative of the egregiousness of the invasion—would collapse the first inquiry into the second. Moreover, courts have rejected invasion of privacy claims related to data equally as sensitive as the data here. *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127–28 (N.D. Cal. 2008) aff'd, 380 Fed. App'x 689 (9th Cir. 2010) (finding no invasion of privacy for disclosure of social security numbers).

J. Plaintiffs' Opposition Does Not Cure The Defects Of Their Deceit Claim

Plaintiffs offer no valid justification for the defects of their deceit claim as laid out in Plaid's Motion. In particular, Plaintiffs rehash the same meritless theory of reliance that they use in connection with their UCL fraudulent claim. But again, Plaintiffs cannot claim they would have acted differently if armed with allegedly omitted information, when the information was in fact available to them. *Davis,* 691 F.3d at 1163 (dismissing fraud claim because plaintiff was able to discover the terms of a contract but refused to read it).

K. Unjust Enrichment is Not an Independent Cause of Action

As Plaintiffs' cited case notes, "in California, there is not a standalone cause of action for 'unjust enrichment', which is synonymous with 'restitution'." *Astiana v. Hain Celestial Grp., Inc*., 783 F.3d 753, 762 (9th Cir. 2015) (citations omitted). As discussed in Section D, Plaintiffs have an adequate remedy at law and do not demonstrate why restitution is needed to make them whole. *Williams,* 2020 WL 6743911, at *9 (dismissing equitable claims where plaintiffs had an adequate remedy of law). Moreover, to the extent the Court treats this as a quasi-contract cause of action based on Plaintiffs allegation of fraud, it fails because Plaintiffs fail to adequately plead reasonable reliance on Plaid's alleged misrepresentation or omission, as discussed above.

III. CONCLUSION

The CAC fails in its entirety for the foregoing reasons, and it should be dismissed with prejudice because Plaintiffs have been unable to plead viable claims despite multiple opportunities to do so across multiple complaints leading up to the CAC.

Dated: December 11, 2020

COOLEY LLP

By: */s/ Whitty Somvichian*
Whitty Somvichian

Attorneys for Defendant
Plaid Inc.

239648460